

MM

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

**IN THE MATTER OF THE SEARCH
VARIOUS ITEMS OF PROPERTY IN THE
CUSTODY OF HOMELAND SECURITY
INVESTIGATIONS, AND LOCATED AT
COMPUTER FORENSIC LABORATORY,
7155 COLUMBIA GATEWAY DRIVE,
COLUMBIA, MARYLAND**

19 - 1718 JMC

Case No. _____

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Augustus Aquino, (sometimes referred to herein as your Affiant) being duly sworn depose and say that:

AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), and formerly known as the United States Customs Service. I am currently assigned to the Office of the Special Agent in Charge in Baltimore, Maryland. I have been so employed since June 1991. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256)¹ in all forms of media including computer media.

¹ "Child Pornography" means "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computer-

19 - 1 7 1 8 JMC

I have also participated in the execution of search warrants, which involved child exploitation and/or child pornography offenses. I am currently assigned to the Maryland Internet Crimes Against Children Task Force (ICAC) which is administered by the Maryland State Police. The ICAC task force was formed to combat the online exploitation of children in the State of Maryland.

2. I have received formal training from U.S. Customs and HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material and Internet crime.

3. As a federal agent, your Affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to effect arrests and execute warrants issued under the authority of the United States.

4. This affidavit is being submitted in support of a search warrant for the computers, hard drives, cell phones and removable computer media (more particularly described in Attachment A) currently located at the offices of U.S. Department of Homeland Security, Homeland Security Investigations (HSI), Computer Forensic Laboratory located at 7155 Columbia Gateway Drive, Columbia, Maryland. The computers, along with hard drives, and media were seized on May 2, 2019, pursuant to a state search warrants executed at 24 Lyndale Avenue, Nottingham, Maryland 21236 (hereinafter the "SUBJECT RESIDENCE") and issued by the Honorable Wayne A. Brooks, Judge for the District Court of Howard County, Maryland. The computers, external hard drives and other removable media were seized from the SUBJECT RESIDENCE from the resident identified as Stephen CORMACK. Several of the devices were also seized from CORMACK's office located at

generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8).

19 - 1 7 1 8 JMC

301 West Preston Street, Office C, 14th Floor, Baltimore, Maryland 21201 (hereinafter the "SUBJECT OFFICE") pursuant to a separate search warrant issued by the Honorable Wayne A. Brooks, Judge for the District Court of Howard County, Maryland.

5. Your affiant has probable cause to believe the computers, hard drives, cameras, and other removable media contain evidence of violations of Title 18, United States Code, Section 2252A(a)(2) (Receipt of Visual Depictions of Minors Engaged in Sexually Explicit Conduct); and Title 18 U.S.C. Section 2252A(5)(B) (Possession of Visual Depictions of Minors Engaged in Sexually Explicit Conduct). These items to be searched are described below and with particularity in Attachment A.

6. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of the aforementioned federal statutes are located within the computers, hard drives, cameras, and other removable media currently held at the offices of HSI and seized from the SUBJECT RESIDENCE and SUBJECT OFFICE.

7. The information contained in this affidavit came from my own participation in the inquiry described herein, as well as from other law enforcement officers, including the Maryland State Police and other third parties in each instance I have identified the sources of information upon which I have relied.

**SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS
AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND
THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION
OF CHILD PORNOGRAPHY**

19 - 1 7 1 8 JMC

8. Based upon your Affiant's experience in child exploitation investigations and upon information provided to your Affiant by other law enforcement officers, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in

19 - 1 7 1 8 JMC

child pornography. This data is typically in digital format, and often maintained on computers and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms, have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

h. Child pornography, or recorded data relating to its transmission, receipt, or distribution that are stored in computer data format, that have been deleted to defeat law enforcement evidence collection efforts, can be recovered by various methods during a forensic examination of the computer system.

FACTS AND CIRCUMSTANCES OF THE INVESTIGATION

9. On February 1, 2019, the Maryland State Police Internet Crimes Against Children Task Force (ICAC) received information that an employee of the Maryland State Department of General Services was allegedly observed by a co-worker ("Witness 1") viewing child pornography at his office located at 301 West Preston Street, Baltimore, Maryland 21201. The employee was identified as Stephen CORMACK.

10. Witness 1 was interviewed by TFC Frank Donald of the Maryland State Police ICAC. Witness 1 described the image as depicting an approximately 8-year-old minor male in underwear but no nudity. Witness 1 described the minor as looking scared in the image. Witness 1 stated that when Witness 1 walked into CORMACK's work cubicle, CORMACK immediately minimized the computer screen. Witness 1, who has known CORMACK for approximately 20 years, stated the

image was not of CORMACK's children. Witness 1 knows CORMACK resides with his wife in Baltimore County, Maryland and has two adult children.

11. Witness 1 further stated the following in substance: Witness 1 had learned years ago that CORMACK had a conviction listed on the Maryland Judiciary Case Search for a sex offense or, as Witness 1 described, "distribution of pornography to children." Witness 1 heard this from another co-worker who had researched it on the Maryland Judiciary Case Search. Over the years, Witness 1 has noticed "suspicious" behavior on the part of CORMACK involving computers. In one situation, Witness 1 observed CORMACK viewing a suspicious website on his personal computer and observed the title "young Japanese boys" on the site. Witness 1 did not see any images at that time. CORMACK immediately minimized the computer screen. Witness 1 has observed CORMACK move from his work computer to his personal laptop computer back and forth during the day. CORMACK also keeps his personal computer where it cannot be readily observed and closes the display whenever someone approaches. Witness 1 has observed this type of behavior by CORMACK over the years and expressed regret over not coming forward sooner with the information. CORMACK always takes his personal laptop to and from work, and a "backup" drive goes home with CORMACK every night.

12. On February 7, 2019, TFC Donald conducted a check of Maryland Motor Vehicle Administration (MVA) records and determined that CORMACK currently resides at 24 Lyndale Avenue, Baltimore, Maryland 21236 (SUBJECT RESIDENCE). TFC Donald caused a subpoena to be issued to Verizon and on February 20, 2019, Verizon responded and advised that an active account existed for Stephen CORMACK at the SUBJECT RESIDENCE.

13. A check of Maryland Judiciary Case Search determined that CORMACK has a

19 - 1 7 1 8 JMC

conviction in Baltimore County, Maryland in 1996 for a second- degree sexual assault. Your affiant has reviewed the file and determined that several victims (now adults) reported they had been sexually assaulted as minors by CORMACK while CORMACK was working at the Parkville Recreation Center.

14. On March 28, 2019, TFC Donald along with Maryland State Police computer forensic examiners accessed CORMACK's office located at 301 West Preston Street, Baltimore, Maryland 21201, specifically labeled "C" and "Steve Cormack" (SUBJECT OFFICE). The Maryland Department of Information Technology provided consent to the Maryland State Police to access the department computer devices located in CORMACK's office. When the Maryland State Police computer forensic examiners logged onto CORMACK's work computer pursuant to the consent and as an administrative logon they encountered the following warning banner:

WARNING: This computer system is for authorized users only. Unauthorized access to this computer is a violation of Article 27, Sections 45A and 146 of the Annotated Code of Maryland. Use of this computer, including e-mail, is monitored. The Office of the Attorney General has the right to inspect, without notice to the user, any work created, including all e-mail messages sent or received, on this computer. Unauthorized use of this computer system may result in disciplinary action. Since security cannot be guaranteed, e-mail should not be used to send confidential information. Questions regarding use of this computer should be directed to the Office of the Attorney General, Information Systems Unit, 200 Saint Paul Place, Baltimore, Maryland 21202 or call 410-576-7838.

The consent included a computer and external hard disk drive used by CORMACK at his work station. During a preview of the devices, Sgt Cooper, Maryland State Police Digital Forensic Examiner, observed an image depicting a minor African-American male approximately 14 to 15 years of age holding his genitals or masturbating. The image was located in the "recycle bin" of the

19 - 1 7 1 8 JMC

external hard drive. The devices were imaged and replaced on CORMACK's desk.

15. On April 18, 2019, Sgt Bedell, Maryland State Police Computer Forensic Examiner, continued a review of the image of CORMACK's work computer that was obtained on March 28, 2019, with the consent of the Maryland Department of Information Technology. Sgt Bedell observed that the Internet browser history on CORMACK's work computer included the website <https://www.stopitnow.org/ohc-content/defining-child-sexual-abuse-material>. Review of the website revealed discussion of the topic of "Defining Child Sexual Abuse Material." One subsection of the website states "Six things you can do if you are concerned about someone else's sexual activity online or use of illegal images." The Internet browser history on CORMACK's work computer also included several websites that detailed police investigations where individuals were charged for child pornography related crimes. For example, one news article was titled "Computer tech uncovers child porn on man's hard drive, police say." Also on April 18, 2019, Sgt Cooper and Sgt Bedell found that Internet search history on CORMACK's work computer included searches for "child porn" on twelve separate occasions on March 8, 2018. Sgt Cooper also found a search of Youtube for "boys skinny dipping" on September 9, 2018. The forensic examiners also observed images of shirtless and scantily clad prepubescent minor males. These images were observed in the "My Documents" folder on the computer.

16. On April 26, 2019, TFC Donald conducted surveillance of the SUBJECT RESIDENCE and observed an elderly Caucasian male exit the SUBJECT RESIDENCE carrying a travel bag. TFC Donald described the male as approximately 6 feet in height with grey hair and weighing approximately 200 lbs. The male entered a Ford Five Hundred sedan bearing Maryland registration 6CAM97. TFC Donald determined through a MVA query of this vehicle that it is

19 - 1 7 1 8 JMC

registered to Stephen Wayne CORMACK and Susan Todd Cormack at the SUBJECT RESIDENCE.

17. On May 2, 2019, Maryland State Police assisted by HSI Special Agents executed state search warrants at the SUBJECT RESIDENCE (CORMACK's residence) and the SUBJECT OFFICE (CORMACK's work space). During the execution of the search warrants, numerous digital devices and other items were located and seized, are the subject of this search warrant, and are more particularly described in Attachment A.

18. CORMACK was read Miranda warnings, waived his Miranda rights, and agreed to be interviewed. CORMACK was asked for the location of the travel case he generally carries from home to work every day. CORMACK stated that the briefcase he ordinarily takes to work with him was located in his car, a Ford which was parked in front of his house. CORMACK stated that the briefcase contained two external hard drives, and one of the hard drives contained a back-up of the files in which he archives for work. CORMACK stated that he does this out of caution since files contained on the office network server have been lost in the past. CORMACK stated that the other hard drive contains photos of family and vacations and personal documents. CORMACK denied there was any "pornography" on this hard drive. CORMACK was advised child pornography had been located on a digital device at his office and that it had been determined he had used Google to search for "child porn." CORMACK denied having used his work computer to look at child pornography but admitted he had used Google and, if child pornography came up, he would look at it. CORMACK admitted he had a personal laptop computer at work and that it should be located in his office either on the desk or in a grey cabinet. CORMACK stated it was an Acer laptop computer and he usually does not bring it home. CORMACK stated that he has the personal laptop at his work site because he has a color printer he uses to print out pictures of family and vacations to display in

19 - 1718 JMC

his office. CORMACK denied producing or distributing or even saving any child pornography but admitted he had looked at child pornography. CORMACK stated he went on “Google at work” to look at child pornography and did not remember any search terms or used any specific “sites.” CORMACK stated “if it comes up, I might look at it.”

19. During the execution of the search warrant at the SUBJECT RESIDENCE, a desktop computer, several CDs/DVDs, and several VHS tapes were located and seized. Additionally, a Ford Five Hundred bearing Maryland registration 6CAM97 and registered to CORMACK located on the street in front of the SUBJECT RESIDENCE was searched, and a notebook and numerous digital devices were located and seized, including the two hard drives CORMACK stated would be in his vehicle (which he transports to and from work), several USB thumb drives, and additional hard drives.²

20. In addition, a search warrant was executed at the SUBJECT OFFICE. During the execution of this search warrant, two digital cameras, several SD cards, CDs/DVDs, a USB jump drive and a Dell laptop computer were located and seized. The Acer laptop computer that CORMACK stated he used to print pictures at the office was also located and seized. The work external hard drive and a Dell desktop computer that were the subject of the consent search conducted by Maryland State Police on March 28, 2019 were also seized.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that digital devices can store information for long periods of time. I also know that digital devices, such as computers, hard

² These items were retrieved and seized from CORMACK’s vehicle and previewed by computer forensic examiners on the day of the execution of the search warrant. The results of this preview are not included in this application.

19 - 1718 JMC

drives, DVDs/CDs, USB thumb drives and digital cameras seized from CORMACK's residence, vehicle and workplace, can be installed or attached to other computers or devices to transfer data, including videos and images.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the electronic devices that are the subject of this warrant because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, transferred to another device and show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other

19 - 1 7 1 8 JMC

information stored on the electronic device and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to produce child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the electronic devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion into a premises. Consequently, I submit there is reasonable cause for the Court to authorize

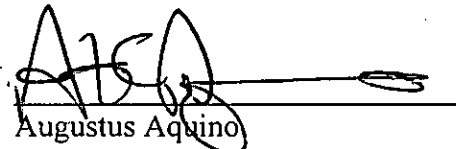
19 - 1 7 1 8 JMC

execution of the warrant at any time in the day or night.

CONCLUSION

25. Based on the foregoing, your Affiant respectfully submits that there is probable cause to believe that Title 18, United States Code, Section 2252A(a)(2) and (a)(5)(B) have been violated and that there is probable cause to believe that evidence of these crimes can be found on the computer, hard drives, various DVDs and CDs, USB thumb drives, digital cameras, and other media more particularly described in Attachment A.

26. In consideration of the foregoing, I respectfully request that this Court issue a search warrant to search the items described in Attachments A which is incorporated herein by reference, and to seize any items located pursuant to the search as described in Attachment B, which is incorporated herein by reference.


Augustus Aquino
Special Agent
Homeland Security Investigations

Subscribed to and sworn before

me this 15 day of May, 2019


THE HONORABLE J. MARK COULSON
UNITED STATES MAGISTRATE JUDGE

FILED _____ ENTERED _____
LOGGED _____ RECEIVED _____

MAY 23 2019

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ DEPUTY

19 - 1 7 1 8 JMC

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

The items to be searched are currently located at the offices of U.S. Department of Homeland Security, Homeland Security Investigations (HSI), Computer Forensic Laboratory located at 7155 Columbia Gateway Drive, Columbia, Maryland, and more particularly described as follows:

The following seized from 24 Lyndale Avenue, Nottingham, Maryland 21236 on May 2, 2019:

- a. Black Toshiba All in One Desktop Computer S/N YC295515Q*
- b. 30 CDs/DVDs*
- c. 2 VHS tapes*

The following items seized from the Ford Five Hundred bearing Maryland Registration 6CAM97 and parked in front of 24 Lyndale Avenue, Nottingham, Maryland 21236 on May 2, 2019:

- d. One spiral notebook and several handwritten notes*
- e. Seagate external 1 TB HDD S/N 2GHHBGFP*
- f. Western Digital Elements HDD S/N WX21AG5P00KV*
- g. Western Digital HDD S/N WXC407165787*
- h. Western Digital HDD S/N WXEY06003970*
- i. PNY 8GB Attache USB Thumb Drive*
- j. Edge Deskgo! 2.0 USB Thumb Drive*
- k. SanDisk Cruzer 4GB USB Thumb Drive*
- l. SanDisk Cruzer Switch 32GB USB Thumb Drive*
- m. SanDisk (Red/Black) USB Thumb Drive*
- n. SanDisk Cruzer Glide 64 GB USB Thumb Drive*

19 - 1 7 1 8 JMC

o. SanDisk Blade 64GB USB Thumb Drive

The following items seized from 301 West Preston Street, Office C, 14th Floor, Baltimore, Maryland 21201 on May 2, 2019:

- p. Grey Acer Aspire Laptop Computer Product Key #*
- q. GH2QR-DH8MX-MV2Y2-P3FQ3-H943B*
- r. 12 SD cards*
- s. Red Lexar Jump Drive 32 MB*
- t. Silver Fantom external HDD S/N*
- u. Dell Desktop Computer Service Tag #7W8GBM2*
- v. Kodak Easyshare DX4000 Digital Camera*
- w. Silver Canon Powershot A300 Digital Camera*
- x. Silver Dell Laptop Computer Service Tag #57Q7D51*
- y. 5 CDs/DVDs*

FILED _____ ENTERED _____
LOGGED _____ RECEIVED _____

MAY 23 2019

BY _____
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND DEPUTY



19 - 1718 JMC

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. All records, documentation, images, videos, or other data contained in the items described in Attachment A, including the following items to be seized which constitute evidence of violations of 18 U.S.C. §§ 2252A(a)(2) and (a)(5)(B):

a. Any and all notes, documents, records, images, videos, text messages, correspondence, calendar entries, or other files referencing or depicting any minor.

b. Any and all visual depictions of other minors engaged in sexually explicit conduct.

c. Any and all correspondence, computer files, or other data identifying persons transmitting, receiving or possessing, through interstate commerce including by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18 U.S.C. § 2256(2).

d. Any and all diaries, notebooks, notes, and any other records reflecting personal contact with or communications about any minor.

e. Any and all records relating to persuading, inducing, enticing or coercing a minor to engage in any sexual activity in violation of the law.

f. Evidence indicating the user's state of mind as it relates to the crime under investigation within this warrant.

h. Evidence of user attribution showing who used or owned the electronic devices described in Attachment A or any predecessor devices replaced by the devices described in Attachment A at the time the things described in this warrant were produced, created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

2. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

19 - 1718 JMC

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER; documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- h. contextual information necessary to understand the evidence described in this attachment; AND
- i. image and video files that depict children engaged in sexually explicit conduct pursuant to Title 18 U.S.C. § 2256.

3. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

19 - 1 7 1 8 JMC

- c. "scanning" storage areas to discover and possible recover recently deleted files;
- d. "scanning" storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.